Pelion Connectivity Management

Security Measures

1. General Description of Pelion's Security Measures

Pelion's security measures are designed to:

a. ensure the security, integrity and confidentiality of Customer Data;
b. protect against anticipated threats or hazards to the security or integrity of Customer Data; and
c. protect against unauthorized access to or use of Customer Data that could result in substantial harm or inconvenience to the person that is the subject of Customer Data.

2. General Procedures

a. Data Storage. Customer Data is always protected using cryptographic means whenever the interfaces to it cannot be properly enumerated and protected, such as when being transmitted over a network. When the data resides in a secure location, such as on servers that are adequately controlled, it is protected using logical means as are known in the art, such as: database access lists and file system permissions. When using cryptography, only established and/or NIST-approved algorithms and modes of operation are being used; for example, symmetric encryption is done using AES-256, and transport encryption is carried out using TLS and DTLS. Customer Data that is stored on Internet-facing hosts is protected by an appropriate border gateway security device, which enforces a strict rule-set on incoming traffic. Anomalous activities, such as activities which can be indicative or an emerging attack, are logged and signalled to the Pelion Security Operation Center for analysis and remediation.
b. Data Transfers. Pelion uses HTTPS standards to protect data integrity during transfers. In addition, subject to Clause 2.a above, Pelion will maintain at least the following security measures: HTTP with TLS 1.2 encryption (HTTPS); and secure access to the Service. Access and Use Monitoring. Pelion will monitor Pelion's user access to and use of the Service for security, performance evaluation, and system utilization purposes.

3. Security reviews of the operations environment

The operations environment is repeatedly reviewed both in terms of design and in terms of actual execution. The latter is accomplished using penetration tests that are carried out by external service providers engaged by Pelion. A summary of outcomes of those reviews can be shared with Customers in certain situations and under certain conditions (such as: exposing just as long as the exposure of the outcome to one customer cannot potentially jeopardize the security posture of another customer).

Pelion has experience in supporting external audits by third parties on behalf of customers. In such situations, some of the internal security review material can be shared with the external auditor, to facilitate a more thorough review for lesser costs.

4. Network security

Network security is a wide security domain that is addressed at multiple levels, some of which are:

a. Reliance on accredited and certified cloud providers to assure, inter alia, secure physical resources.
b. A strong dedicated border gateway (a.k.a., 'firewall') through which all traffic is routed, and which can deal with encrypted traffic.
c. Patch management and vulnerability management: the former deals with knowing when components that the overall system relies on need to be updated and carrying out such updates; the latter refers to the lifecycle of discovered vulnerabilities from their discovery to their remediation, along with the associated risk management.
d. Secure authentication through use of multiple authentication factors and implementation of role-based mapping of privilege to the capability of the assigned administrator. Authentication mechanisms rely on a centralised directory server where the aforementioned mappings occur and

multi-factor authentication at the network edge. Proper logging of both successful and failed attempts, along with the alerts to the Pelion Security Operation Center.

e. Secure administrative remote access to the service network, such as by using a VPN endpoint to secure incoming network connections for administration.
f. Tier-1 third party data centre providers, where Pelion equipment is hosted and used to transit Device Data to private networks or the internet.
g. g. Fixed-line connectivity providers, that are used for the interconnect between Pelion and mobile network operator (MNO) partners which is used for the private transit of Device Data.
h. h. MNO partners, who are managed as third party suppliers that meet minimum security principles for device usage on their network.
i. i. SIM and RSP suppliers, who manage the generation and storage of secure keys for network attach and the manufacturing of physical SIM form factors.

5. Backup and Business Continuity

Pelion maintains a business continuity program, including a recovery plan, sufficient to ensure Pelion can continue to function through an operational interruption and continue to provide the Service to Customer. The program provides a framework and methodology, including a business impact analysis and risk assessment process, necessary to identify and prioritize critical business functions. In the event Pelion experiences an event requiring recovery of systems, information or services, the recovery plan will be executed promptly. Pelion continuously enhances the Service's security and availability of its multi–tenant enterprise class cloud-based and hosted infrastructure. Pelion maintains means of being able to recover copies of Customers Data and tests those regularly.

6. Key Management

Encryption keys are used all around the hosted software application used to provide the Service. They are used for secure storage, for token generation, for authentication and AKE algorithms. The hosted software application used to provide the Service does not utilize a single centralized key-store, for both architecture and security reasons. Different keys are stored by different means in accordance with their availability and security requirements.

See below for a few examples for keys in the system and their storage:

a. The highest-grade keys are the keys used in the internal certification authority. Those keys are implicitly trusted by all components and are expensive to ever replace. Those keys are stored offline to prevent use outside designated renewal operations.
b. Private keys that are used by different hosts to authenticate (only) themselves maybe be stored by the hosts, with proper file-system permissions.